THE NATIONAL CYBERSECURITY SOCIETY

How To Select a Managed Security Service Provider

The NCSS recommends small businesses acquire a Managed Security Service Provider (MSSP) to protect your data, systems and access to online resources. A MSSP is defined as an IT service provider that delivers multiple security services – such as virus and spam blocking, intrusion detection, continuous monitoring, firewalls and/or virtual private network (VPN).

A MSSP manages security for an organization as either a monthly service fee or by the number of employees serviced.

The unique value in using a MSSP, is this provider takes the burden off of the small business in managing security system changes, new configurations, and staying abreast with the latest security threats. Some MSSPs offer services for regulated industries such as health care and financial as well as provide compliance with GDPR.

In most cases, a MSSP provider will be more cost effective than acquiring in-house IT security staff. However, you will still need to be able to discern what services to acquire because ultimately a data breach or cyber-attack is still your responsibility.

STEP 1: Define your requirements

This might be a hard step for most small businesses, so we have made it easy by defining the minimum set of capabilities your business should require from a MSSP. The MSSPs that are listed under our Member Perks page are companies that the NCSS has evaluated for applicability in terms of cost and approach. Before you consult with a MSSP, you should determine which compliance regime you either are governed by or want to follow.

Some suggested compliance regimes are:

1. HIPPA
2. NIST 800-171
3. SOC 2 GDPR
4. PCI DSS

Did you know?

√ Do you know what IT security frameworks govern your business?

√ A MSSP is more cost effective than trying to do IT security on your own

√ Identify a company POC who can interact with your MSSP account manager - a MSSP is an extension of your staff

√ Some MSSPs provide VPN services

√ When you decide to acquire the services of a MSSP, check out our list of companies under Member Perks

Still have questions, need help?

Contact us at our "**Ask-an-Expert**" service, **web@thencss.org** or visit us at the link below.

How to Select a MSSP continued…

Voluntary Framework to consider:

1. NIST Cybersecurity Framework
2. ISO 27001
3. NIST Risk Management Framework

The minimum requirements for an MSSP include:

- 24/7/365 Security Operations Center capabilities
- Incident Response
- Vulnerability Assessments/Continuous Monitoring (preferred)
- Security Incident and Event Monitoring (SIEM)
- Network Intrusion Detection System (IDS), Host IDS
- Change Detection - file integrity monitoring
- Compliance Monitoring and Reporting

STEP 2: Identify a Company Lead and Budget

Next step is to Identify who in your company will be the interface with the MSSP. This staff member will ultimately be your project manager to select, acquire and transition to a MSSP. Concurrently, your organization should identify the resources to pay for the MSSP. There may be an initial cost of onboarding, then a monthly fee based upon the size of your infrastructure. Costs range from $3000 - $10,000/year.

STEP 3: Initial Assessment

Once you've selected a MSSP, the provider will complete an initial assessment to establish a baseline. This assessment will identify all assets connected to your infrastructure and identify any vulnerabilities or weaknesses in either the controls, software currency, open ports, lack of documentation, etc. The provider should provide you with a project plan with the critical or high deficiencies identified during the assessment. Your MSSP account representative should help you to understand the deficiency, prioritize the remediation and help with estimating time and costs. Resolving these issues may take 3-6 months to correct and may require changes in your network, training staff, or retooling of specific business processes.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

How to Select a MSSP continued...

STEP 4: Operations and Sustainment

Once you are up and operational, expect to receive monthly reports. If you don't understand something, ask. Your company should have an account manager - someone who is there to help your company stay safe and improve operations. Other sustainment activities your company should expect from your provider are: regular account meetings, help desk or ticket management, advice on expanded services - such as backups, phishing training, and/or VPN. Start small and grow as your business expands.

References:

The Industry research firm, Forrester Research, identified the 14 most significant vendors in the global market in 2018 with its 23 elements evaluation of managed security service providers (MSSPs). The MSSP market has matured and several of the industry leaders included Accenture, Alert Logic, AT&T Business, BAE Systems, CenturyLink, Deloitte, IBM, NTT, Optiv Security, Secureworks, Symantec, Trustwave, Verizon, and Wipro. See the full report:

https://www.forrester.com/report/The+Forrester+Wave+Global+Managed+Security+Services+Providers+MSSPs+Q3+2018/-/E-RES141654

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.